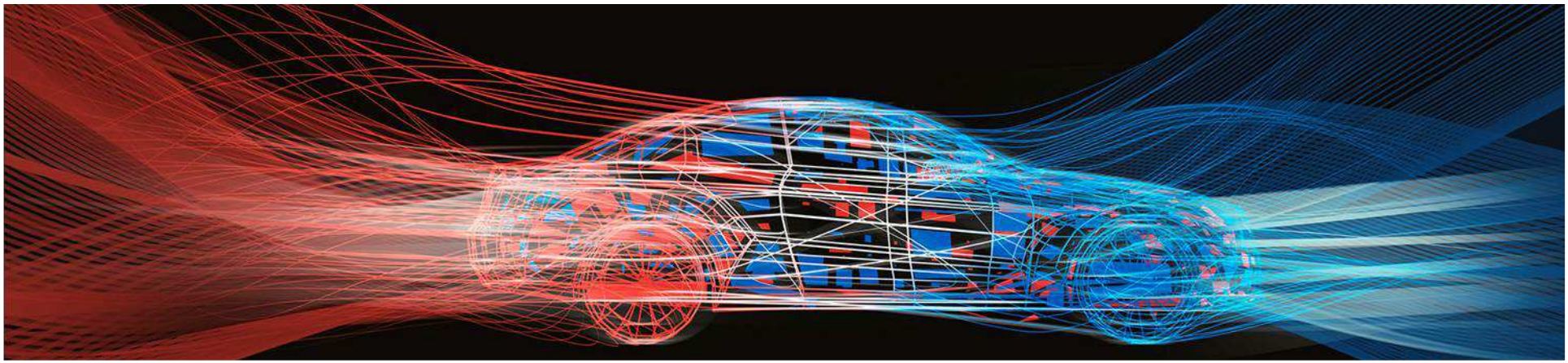
Hardware-Assisted Cyber Security in Automotive Systems

IEEE Hardware Oriented Security and Trust, May 3, 2016

Brian Murray, Director Safety and Security Excellence, ZF TRW

ZF Friedrichshafen AG



ZF and TRW, The Power of 2

ZF Group

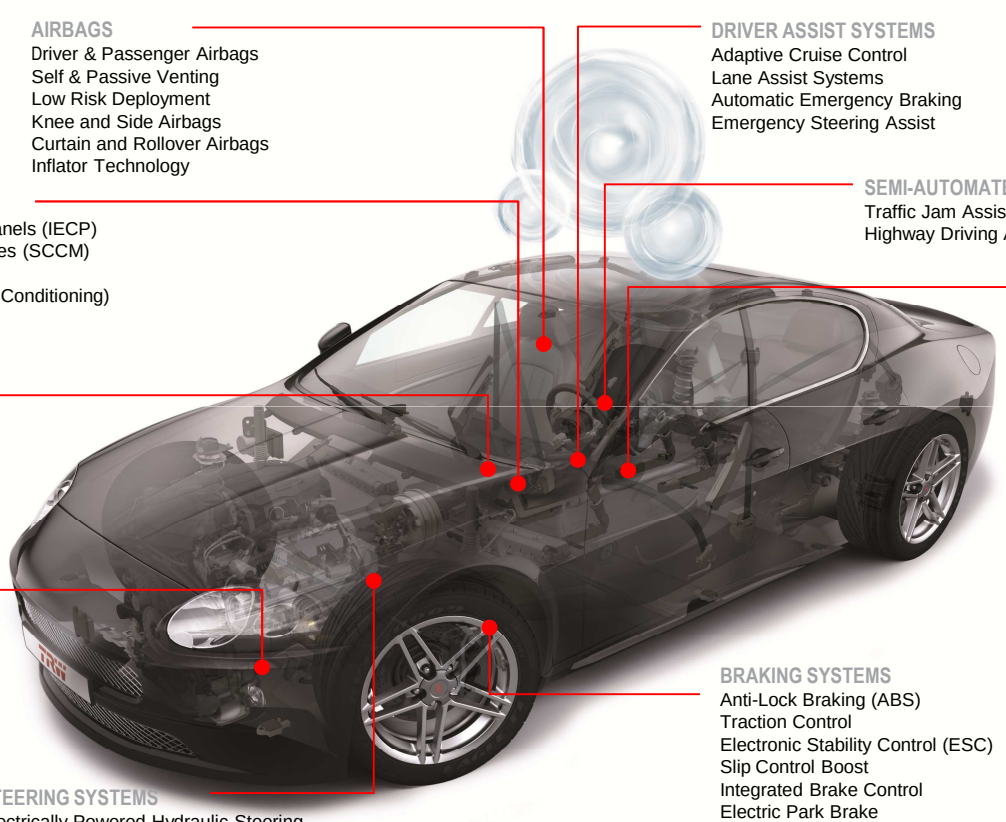
Areas of Activity: Divisions and Business Units

Car Powertrain Technology	Car Chassis Technology	Commercial Vehicle Technology	Industrial Technology	Active & Passive Safety Technology
Automatic Transmissions	Chassis Systems	Truck & Van Driveline Technology	Off-Highway Systems	Braking Systems
Manual/Dual clutch Transmissions	Chassis Components	Axle & Transmission Systems for Buses & Coaches	Test Systems	Steering Systems
Axle Drives	Suspension Technology	CV Chassis Modules	Special Driveline Technology	Commercial Steering Systems
Powertrain Modules		CV Damper Technology	Marine Propulsion Systems	Occupant Safety Systems
Electric Drive Technology		CV Powertrain Modules	Aviation Technology	Electronics
Die Casting Technology			Wind Power Technology	Body Control Systems
ZF Services				Engineered Fasteners & Components
Electronic Systems				Parts & Service

Brands

SACHS LEMFÖRDER BOGE ZF Parts TRW

ZF TRW



AIRBAGS
Driver & Passenger Airbags
Self & Passive Venting
Low Risk Deployment
Knee and Side Airbags
Curtain and Rollover Airbags
Inflator Technology

DRIVER ASSIST SYSTEMS
Adaptive Cruise Control
Lane Assist Systems
Automatic Emergency Braking
Emergency Steering Assist

SEMI-AUTOMATED DRIVING
Traffic Jam Assist
Highway Driving Assist

BODY CONTROL SYSTEMS
Integrated Electronic Control Panels (IECP)
Steering Column Control Modules (SCCM)
Switches and Switch Modules
HVAC (Heating, Ventilation, Air Conditioning)
Sensors
Access Systems

STEERING WHEEL SYSTEMS
Touch Sensor in Steering Wheel Rim
Hands Off Detection
Vibrating Steering Wheel
Illumination Technology
Contactless Horn System
Path-free use of Horn
Steering Wheel with Integrated Microphone
Electrical Connections
Heated Steering Wheel

SEAT BELT SYSTEMS
Active Control Retractor
Seat Belt Retractors
Load Limiters
Pretensioners
Active Buckle Lifter
Buckles

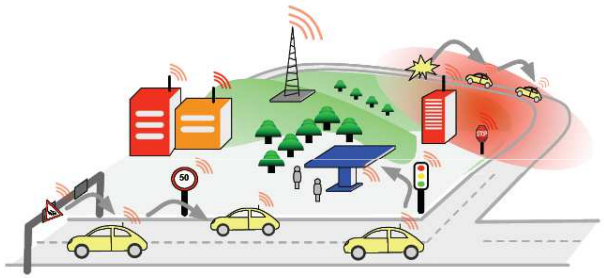
ELECTRONICS
Electronic Control Units
Airbag Control Units
Video and Radar Sensors
Integrated Sensors
Safety Domain ECU
Pedestrian Protection
Crash Sensors
Tire Pressure Monitoring

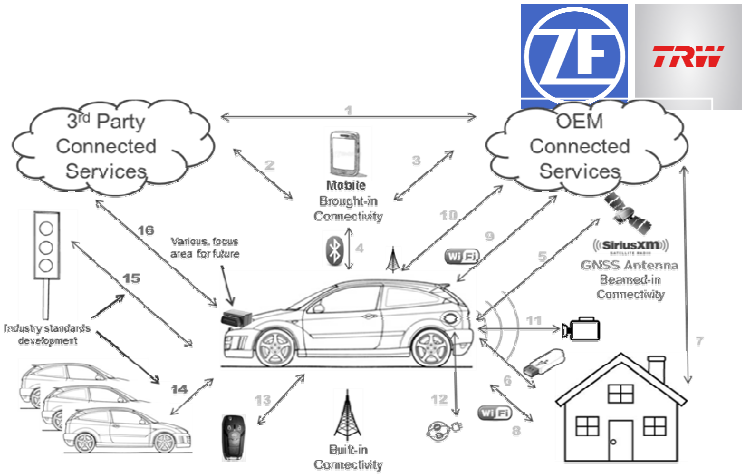
BRAKING SYSTEMS
Anti-Lock Braking (ABS)
Traction Control
Electronic Stability Control (ESC)
Slip Control Boost
Integrated Brake Control
Electric Park Brake
Calipers / Rotors
Actuation

STEERING SYSTEMS
Electrically Powered Hydraulic Steering
Electrically Powered Steering Column Drive
Electrically Powered Steering Rack Drive

Megatrend: Safety

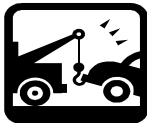
- 32,675 automotive-related fatalities in 2014, > 94% without Vehicle Factors (Source: NHTSA)
- NHTSA believes Active Safety, Autonomous Driving, and Connected Vehicles are an essential part of driving fatalities down





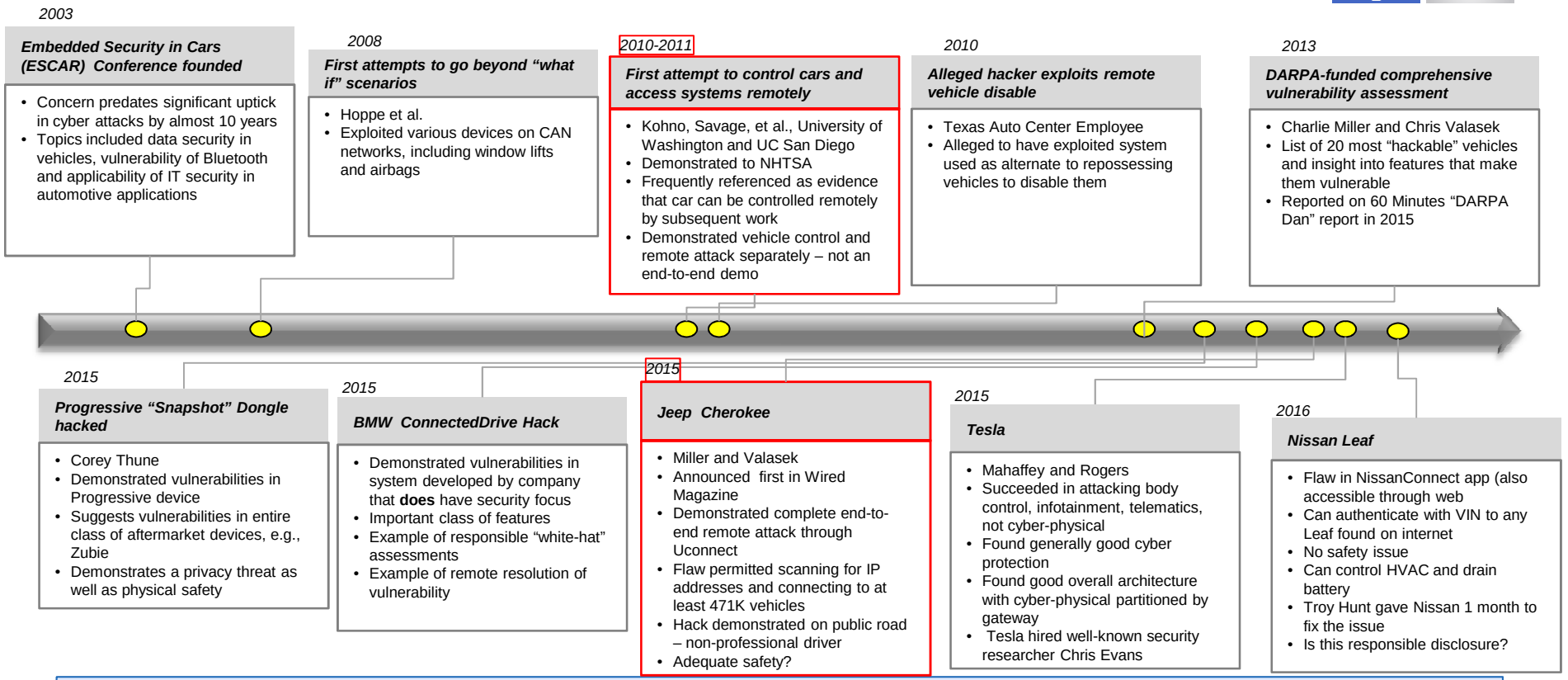
Source: SAFESPOT Project

- Increased interconnectivity of today's and future vehicles makes them potential targets for attack
  - Losses can include: Financial, Operational, Privacy, Safety and Reputation



- **Hacking and recalls erode critical consumer trust in new technologies important to vehicle safety**

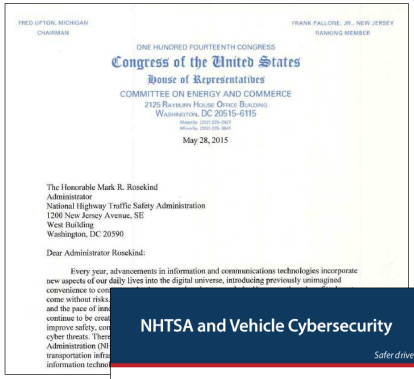
A Brief History of Automotive “Hacking”



Research conducted by “White-Hat” hackers (Security Researchers)
Only one known potential malicious attack in Automotive to date

Other Relevant Automotive Cybersecurity News

- NHTSA under pressure from US Congress to regulate automotive cyber security, legislative action so far
  - Spy Act, House E&C "Re-TREAD" Act Discussion Draft
  - NHTSA has built capability to analyze vulnerabilities
  - Michigan Senate introduced draft vehicle anti-hacking bill May 2, 2016
- The Automotive Industry is taking action on standards
  - SAE published J3061 Cybersecurity Guidebook for Cyber-Physical Automotive Systems, ISO-TC22 N3556 NWIP Automotive Security Engineering
- The Automotive industry also launched an Information Sharing and Analysis Center – AutoISAC
  - Both Association of Global Automakers and Alliance of Automobile Manufacturers
  - Operated and managed by Booze-Allen
- Security research community
  - Still interested in Automotive – Car Hacking Village back at DEF CON for 2016
  - Believe "Openness" is the best strategy, e.g., push for Automotive Exemption to 2015 DMCA update
- EU – Data Protection Directive



FRED UPTON, MICHIGAN
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS

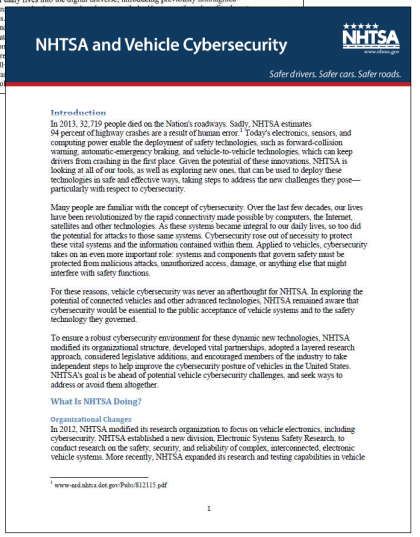
Congress of the United States
House of Representatives
COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

May 28, 2015

The Honorable Mark R. Rosekind
Administrator
National Highway Traffic Safety Administration
1200 New Jersey Avenue, SE
West Building
Washington, DC 20590

Dear Administrator Rosekind:

Every year, advancements in information and communications technologies incorporate new aspects of our daily lives into the digital universe, introducing previously unimagined



NHTSA and Vehicle Cybersecurity

NHTSA

Safer drivers. Safer cars. Safer roads.

Introduction

In 2013, 32,719 people died on the Nation's roadways. Sadly, NHTSA estimates 94 percent of highway crashes are a result of human error.[1] Today's electronics, sensors, and computing power enable the deployment of safety technologies, such as forward-collision warning, automatic-emergency braking, and vehicle-to-vehicle technologies, which can keep drivers from crashing in the first place. Given the potential of these innovations, NHTSA is looking at all of our tools, as well as exploring new ones, that can be used to deploy these technologies in safe and effective ways, taking steps to address the new challenges they pose—particularly with respect to cybersecurity.

Many people are familiar with the concept of cybersecurity. Over the last few decades, our lives have been revolutionized by the rapid connectivity made possible by computers, the Internet, satellites and other technologies. As these systems became integral to our daily lives, so too did the potential for attacks to those same systems. Cybersecurity rose out of necessity to protect these vital systems and the information contained within them. Applied to vehicles, cybersecurity takes on an even more important role: systems and components that govern safety must be protected from malicious attacks, unauthorized access, damage, or anything else that might interfere with safety functions.

For these reasons, vehicle cybersecurity was never an afterthought for NHTSA. In exploring the potential of connected vehicles and other advanced technologies, NHTSA remained aware that cybersecurity would be essential to the public acceptance of vehicle systems and to the safety technology they governed.

To ensure a robust cybersecurity environment for these dynamic new technologies, NHTSA modified its organizational structure, developed vital partnerships, adopted a layered research approach, considered legislative additions, and encouraged members of the industry to take independent steps to help improve the cybersecurity posture of vehicles in the United States. NHTSA's goal is be ahead of potential vehicle cybersecurity challenges, and seek ways to address or avoid them altogether.

What Is NHTSA Doing?

Organizational Changes

In 2012, NHTSA modified its research organization to focus on vehicle electronics, including cybersecurity. NHTSA established a new division, Electronic Systems Safety Research, to conduct research on the safety, security, and reliability of complex, interconnected, electronic vehicle systems. More recently, NHTSA expanded its research and testing capabilities in vehicle

[1] www-nrd.nhtsa.dot.gov/Pubs/812115.pdf

1

Automotive Industry will create Trusted Communities for Cyber Security Support

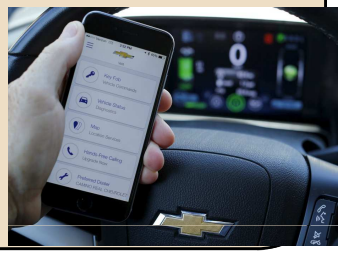
Automotive Threats: The Four Ps

Physical Safety

- Safety hazards that can be caused by malicious attacks
- The most visible example of this is takeover of critical car functions like braking and steering

Physical Security

- Attacks on the car door locks, immobilizer and other physical security features



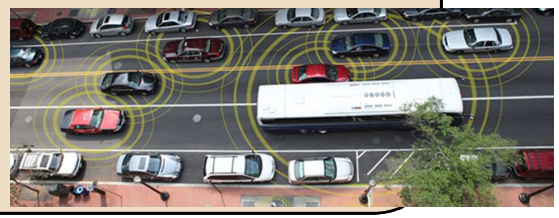
REUTERS/Mike Blake

Personal Information Security

- Attacks intended to extract or leak identity, financial or other private information acquired or managed on the vehicle

Pivot

- Attacks on vehicle systems intended as a precursor (pivot point) to exploit other systems



Automotive Vulnerabilities

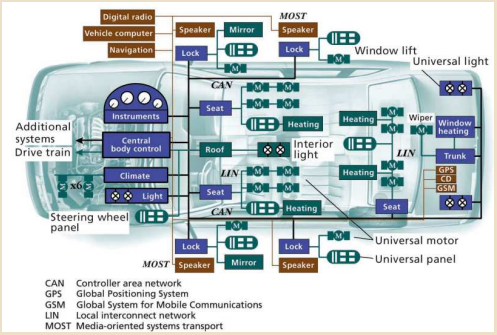
External Cyber Interfaces

- All intentional wired and wireless interfaces, including maintenance interfaces to ECUs and diagnostic interfaces
- Vulnerabilities, examples:
  - Lack of authentication
  - Lack of input checking

Verizon

Cyber Architecture

- Configuration of embedded system devices, including wired and wireless communication channels, protocols, power infrastructure and ECUs
- Vulnerabilities, examples:
  - Lack of authentication handshake
  - Integration of sensitive components with “open” systems

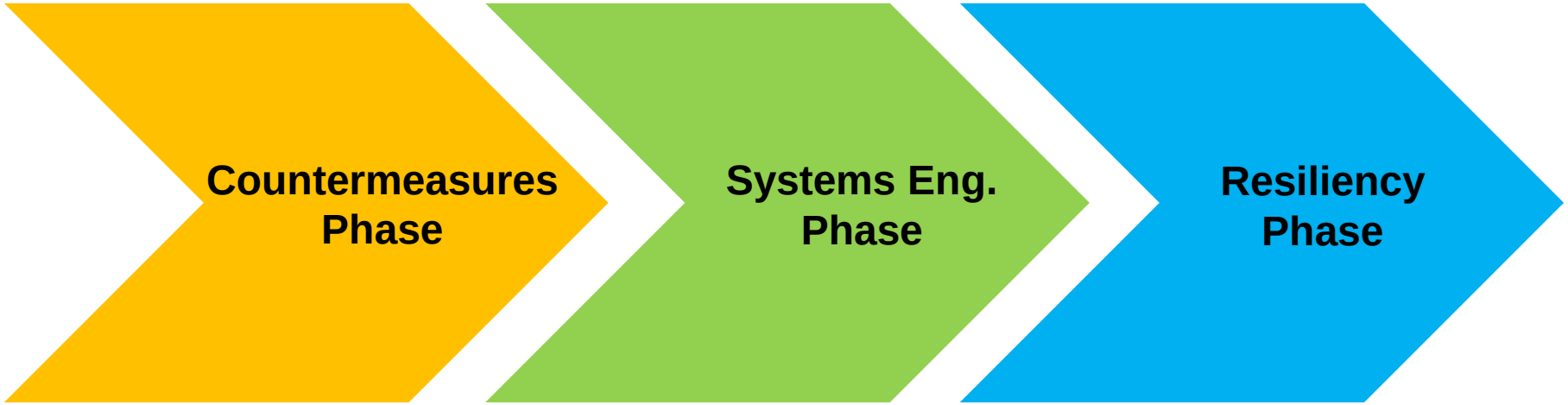


G Leen, et al.

Cyber-Physical

- Embedded systems that control the physical world, electric power steering, brake systems, engine control, remote keyless entry, …
- Vulnerabilities, examples:
  - Software bugs
  - Lack of input checking

Automotive Industry Phases



Today

- Implement basic security infrastructure
- Focus on Enforcing Trust Boundaries

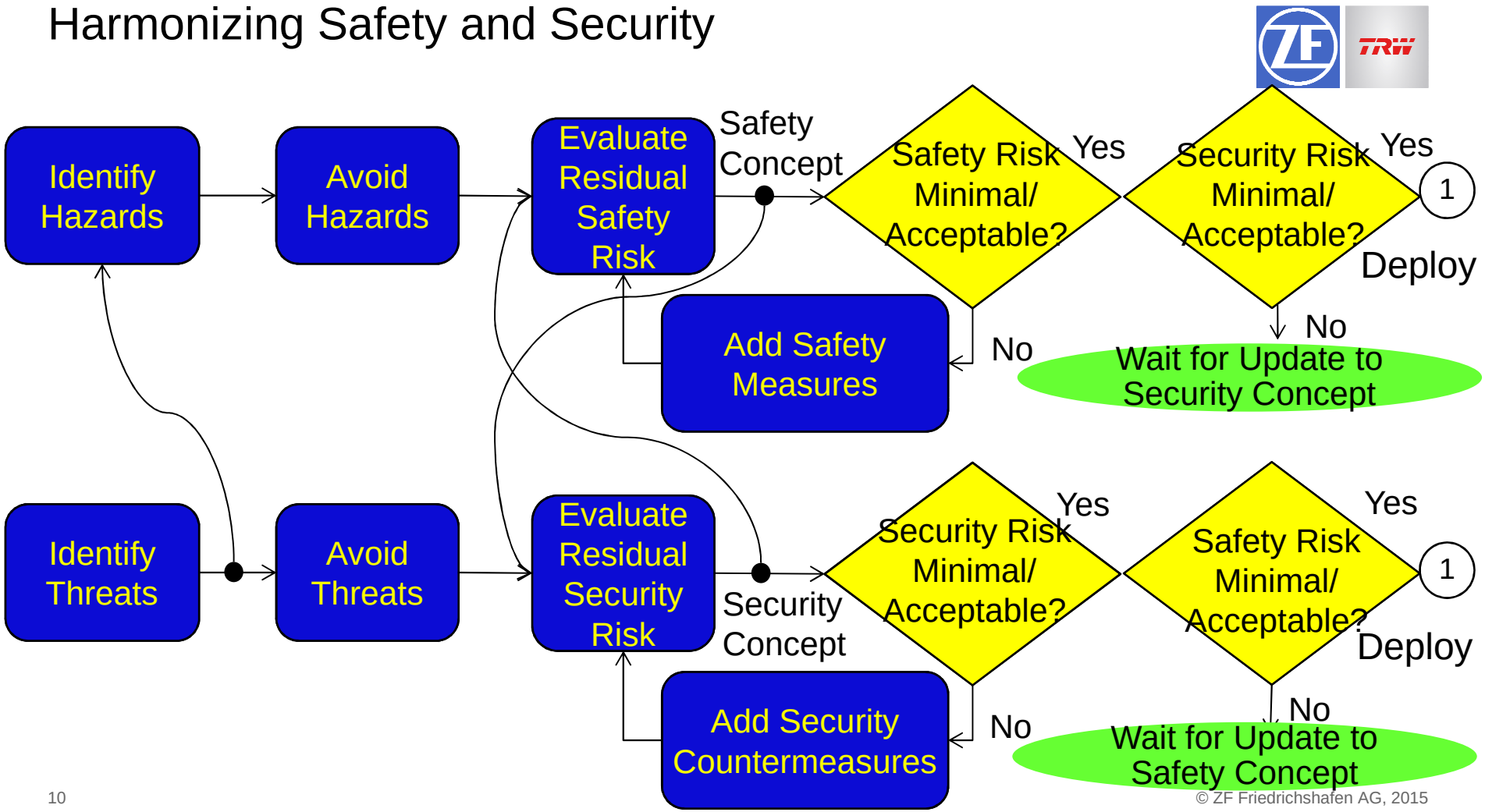
Next

- Implement risk-based security process
- Rationalize countermeasures and trace to requirements

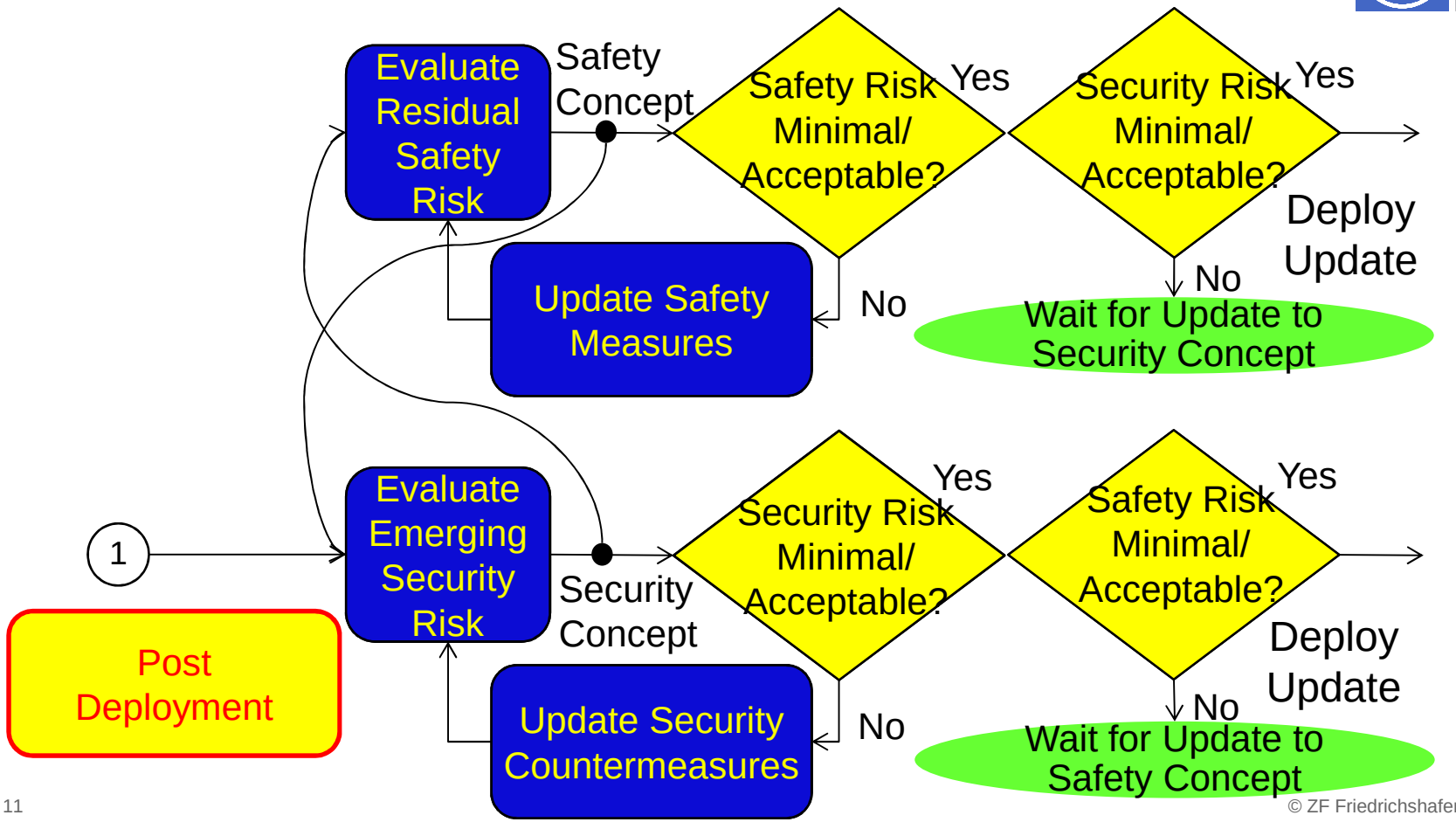
Future

- Provide ability to adapt to be resilient to new threats
- Look beyond single cars to fleets of connected vehicles

Harmonizing Safety and Security

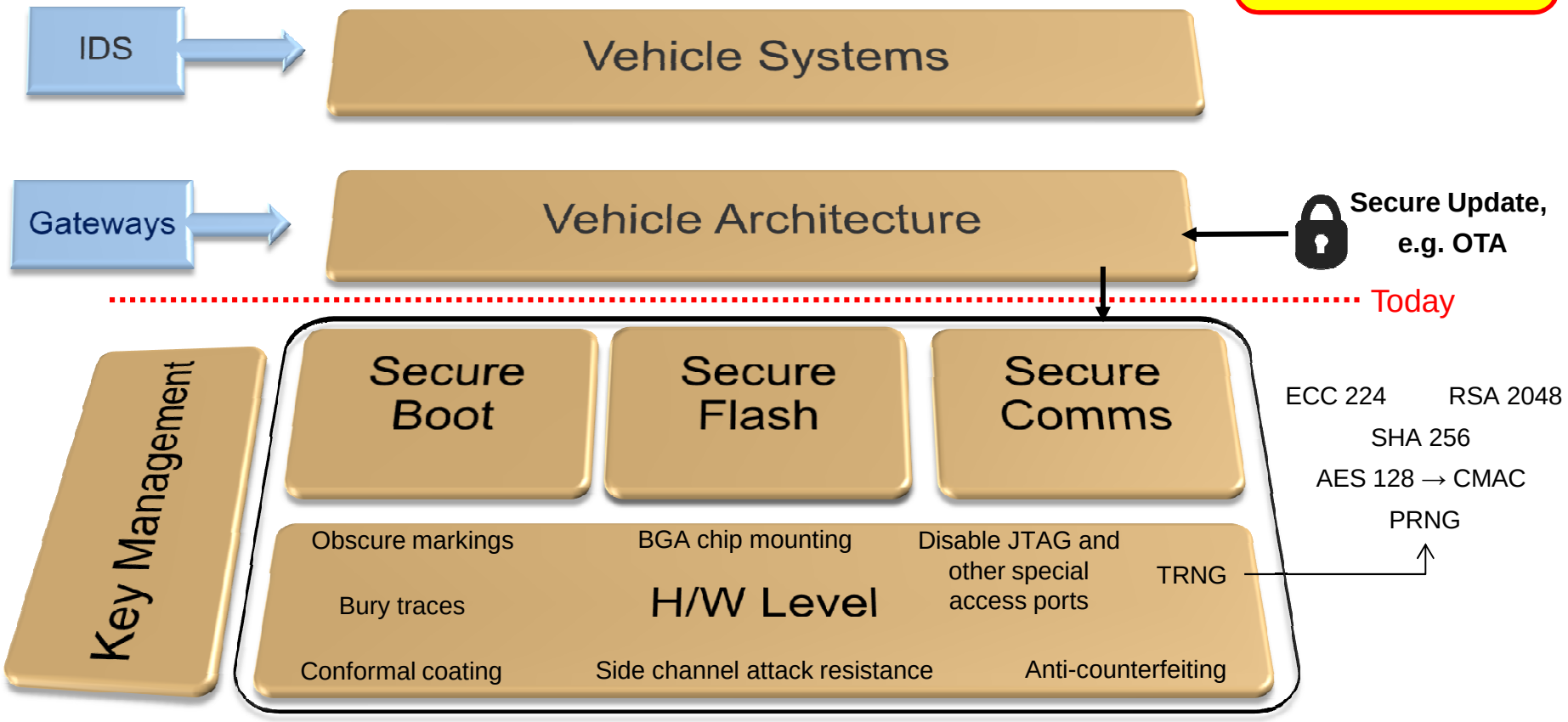


Harmonizing Safety and Security

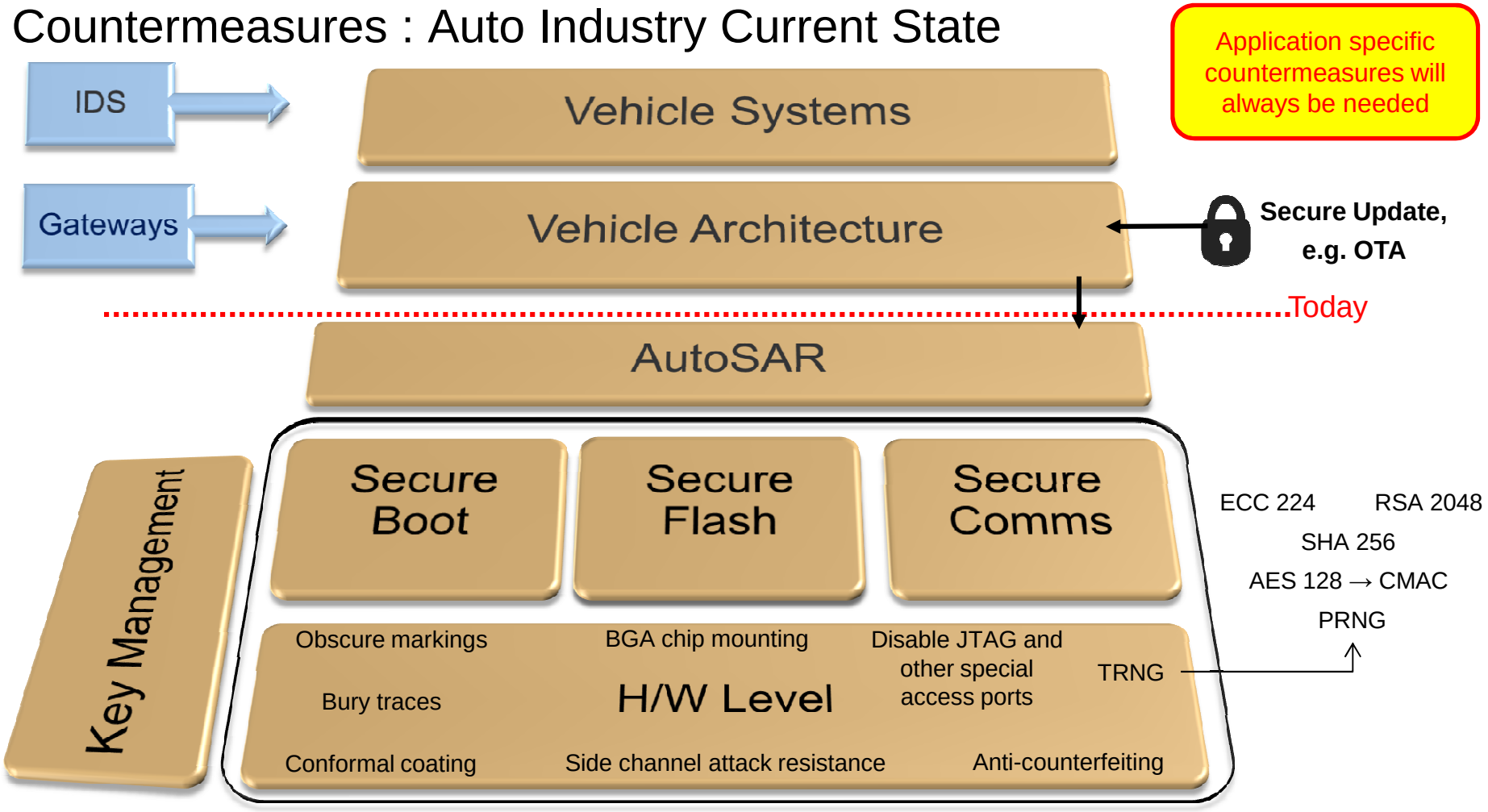


Countermeasures : Auto Industry Current State

Application specific countermeasures will always be needed



Countermeasures : Auto Industry Current State



Automotive Hardware Protected Security – Background

EVITA

- European research project June 2008 –Dec 2011
- **E**-safety **V**ehicle **I**ntrusion pro**T**ected **A**pplications
- http://evita-project.org/index.html
- Design, verify, and prototype an architecture for automotive on-board networks where security-relevant components are protected against tampering and sensitive data are protected against compromise when transferred inside a vehicle
- Key architecture component: Hardware Security Module (HSM) integrated on-chip with micro
  - Full, Medium, and Light versions
  - Full: Symmetric, and Asymmetric Cryptography, Hash, Pseudo-Random Numbers (TRNG seed), Secure Keys Storage, Secure Execution Engine, …
  - Assume attacker will not access inside the chip – protection against side channel attacks and hardware attacks discounted to reduce cost

HIS SHE

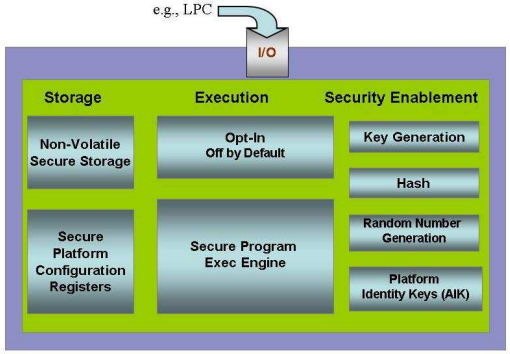
- HIS – Herstellar Initiative Software
- SHE – Secure Hardware Extension
- Among other activities, define functional architecture for an HSM that satisfies EVITA Light HSM
- Features: Secure Keys and Execution Engine, AES 128, CMAC, Miyaguchi-Preneel Compression, …
- Particular attention to Secure Boot

Automotive HSM Status

- Since EVITA, the Automotive Industry has seriously considered Hardware Protected Security and HSMs
  - Primary assumption is that low-cost controllers cannot employ strong security features without hardware support
  - SAE is developing a common set of expectations and requirements – J3101
- Almost all vehicle manufacturers have a strategy that includes Hardware Protected Security
- Almost all semiconductor manufacturers are implementing on-chip, peripheral HSMs or have plans for HSMs
- Most current HSMs conform to SHE or “SHE+” (any features beyond SHE – EVITA “Light” and “Medium”)
  - SHE is a “functional” standard – there is no standardized programming model – nor is there one under development
  - Programming model may be provided by AutoSAR
- Most vehicle manufacturers require features that go beyond SHE, especially asymmetric encryption for certificates, e.g., for software updates
- Most designs are very new
- Drivers and other software supporting HSMs are new

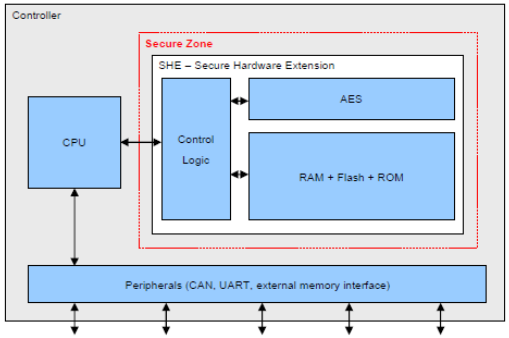
Vendor	Model	Option
NXP	Cobra55	CSE2
NXP	S32	CSEc
NXP	Calypso	HSM
NXP	IMX6	TEE
Renesas	RH850	ICUs
Renesas	RH850	ICUm
ST	Chorus	HSM
TI	Jacinto	TEE
Infineon	Aurix	HSM
Infineon		TPM
Atmel	Border Security Dev	Secure TRx
NXP	S2T	Secure TRx
Oberthur		Euicc

TPM versus HSM – Observations



Trusted Platform Module

- Intended as hardware “Root of Trust”
  - Authentication
  - Attestation
- Typically implemented as standalone chip with significant side-channel protection
- International standard managed by Trusted Computing Group



Secure Hardware Extension

- Intended as hardware-supported set of important security functions
  - **Key features**: secure key storage, secure execution of crypto algorithms, hardware implementation of crypto algorithms and RNG as needed
  - **Anticipated use cases**: secure keystore, authenticated boot, authenticated SW flash, authenticated in-vehicle messaging, broadcast/multi-cast authentication, secure storage, controlled access to private data, secure diagnosis in ECU, vehicle threat protection, IP protection, remote attestation, secure logging, secure erase, anonymization
- Implemented on-chip in microcontroller – threat model assumes hardware attack low-risk
- Function standard under development by SAE

Automotive-inspired HSMs have tremendous potential for IoT security

Some Open Issues

- Simultaneously meeting safety and security requirements with HSMs
  - How do faults affect HSMs?
  - What is error detection capability of HSMs?
- Are there substantial risks from side-channel or other hardware vulnerabilities in current HSMs?
- How will vulnerabilities found in HSMs after deployed be handled?
- Key management strategies for systems employing HSMs
- Performance requirements
  - Rate, timing, power, ...